Remarks of Commissioner Edith Ramirez
Privacy by Design Conference
Hong Kong

A. Privacy by Design

The hallmark of privacy by design is a deliberate and systematic approach to privacy and data security. The FTC framework uses the term privacy by design to include the following:

First and foremost, companies should embed privacy and security into their products and services from the outset. Second, companies should only collect the data they need for a specific business purpose and should safely dispose of it when that objective has been accomplished. Third, companies should employ reasonable security to p

possible. Let me give you a few real-world examples that show the promise of privacy by design if it were to be embraced systematically:

- Appleôs Safari browser blocks third-party tracking cookies by default. This feature is automatically turned on, making it easier for consumers to prevent unwanted tracking of their activity across websites.

-

interaction between the business and the consumer. If a data practice is not consistent with the context of the interaction, choice should be given.

In connection with online behavioral advertising, one way to simplify choice is through ñDo Not Track,ò which is one of the FTCôs most visible privacy initiatives. To the FTC, Do Not Track means a universal, one-stop tool for consumers to permanently opt-out of tracking across websites. We also believe that Do Not Track should go beyond opting consumers out of receiving targeted advertisements. It should stop the collection of data across websites for all purposes other than those that would be consistent with the context of the consumerôs interaction with a website, such as capping the number of times a particular advertisement is shown and preventing fraud.

The FTC first called for Do Not Track in December 2010, at a time when the idea had little industry support. Our call for Do Not Track has since mobilized three key sets of players: the browsers, the U.S. online media and marketing industry, and the technical standards community.

Shortly after the FTC endorsed Do Not Track, Microsoft and Mozilla began to offer browser-based tools for consumers to communicate to websites their desire not to be tracked. Apple Safari and Opera later followed, and recently Yahoo! and Google have announced they will deploy Do Not Track mechanisms in their browsers later this year. Microsoft also recently announced that the next version of Internet Explorer will come with Do Not Track turned on by default.

Of course, a signal from a browser that a user does not want to be tracked is useless if it

program that uses icons in online ads. That program was designed to operate separately from browser-based tools, but in February the DAA committed to honor browser-based choices made by consumers. Major online presences like Twitter have also pledged to adhere to Do Not Track. Importantly, the DAA has also promised to ban its members from transferring online tracking data for use in determining employment, credit, insurance, and health care eligibility. That prohibition addresses a critical privacy concern a number of us at the FTC have expressed. In addition to these efforts, the World Wide Web Consortium or ñW3C,ò an Internet standard setting body, is creating a global technical standard for Do Not Track.

Significant issues remain before the FTCôs Do Not Track vision will been realized. But I am hopeful that we will have a viable Do Not Track system in place in the near future, and I look forward to industryôs continued efforts to make that happen.

C. Transparency

The third principle in the FTCôs framework is transparency. Companies should disclose details about their collection and use of consumer data. As I mentioned, the FTC urges companies to provide simplified choice to consumers beyond lengthy privacy policies. But the FTC does not want privacy policies, which provide a comprehensive, public description of a companyôs data practices, to be eliminated. We do, however, want to see privacy disclosures simplified and standardized so that consumers can compare data practices across companies.

II. Next Steps on the Policy Front

In the next year we expect to tackle several key recommendations in our report. For example, we recently held an FTC workshop addressing how to make effective privacy disclosures on mobile devices. We will update our industry guidance based on the information gathered.

We will also look at what we refer to as large platform providers, such as Internet Service

I Tm[ )]TJ8.74 1 72.024 681.5orm 5rovidopet nsucryservicmvidbr m providh nd soc pria rvicdia. T prhrvic m pr

We also charged Facebook with making misleading statements about the data shared with third-party apps on the site. Facebook told consumers that third-party apps could access only the

B. Google

The FTCôs action against Google involved Googleôs rollout in 2010 of its now-defunct Google Buzz social network.[4] Perhaps in its rush to launch a product to compete with Facebook, Google used Gmail accounts to populate the Buzz social network. In doing so, Google took the frequent contacts of Gmail users, which had been private, and made them public. We charged that this was done without usersô consent and in violation of Googleôs privacy policy.

Significantly, the resulting settlement order applies to the full array of Googleôs many products and services. Under the order, Google cannot misrepresent how it treats consumer data. It also cannot change a product or service in a way that makes consumer information more widely available to third parties without getting consumersô affirmative express consent. As with *Facebook*, each order violation can result in civil penalties of up to $16,000 per day. Collectively, the FTCôs orders against Facebook and Google will benefit well over a billion consumers across the globe.

C. Frostwire

I would also like to tell you about an FTC privacy enforcement action against a lesser-known company called Frostwire.

Frostwire designed mobile P2P software downloaded by hundreds of thousands of individuals on Android devices. Last October, the FTC charged that Frostwireôs Android application caused its users to unknowingly share their pictures and other data.[5] Frostwire had set the default settings to automatically reveal private photos and videos taken with usersô phones to other P2P users around the world. The Frostwire desktop app had never worked that way, and

[4] *See Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (complaint and consent order), *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.
[5] *See FTC v. Frostwire LLC*, No. 11-23643-CV (S.D. Fla. filed Oct. 11, 2011) (complaint and consent order), *available at* http://www.ftc.gov/os/caselist/1123041/111012frostwirestip.pdf.

we alleged that many Frostwire users would not have understood that the photos, videos, and other files on their phones would be automatically shared. We charged that Frostwireôs configuration of the mobile app in this way was an unfair practice.

Had Frostwire practiced privacy by design, it would have built its mobile app to guard against the unwanted sharing of private photos and other personal files with an entire P2P network. As a result of the FTCôs lawsuit, Frostwire must now do so. Under a settlement order entered by a court last fall, Frostwire cannot use default settings that automatically share the files users have created. In other words, the order helps ensure that going forward Frostwire will follow privacy by design.

IV. APEC and Cross-Border Data Transfers

I would now like to turn to cross-border privacy issues and the role that privacy by design can play in that arena. Consumer data can now be transferred around the globe in the blink of an eye. That reality demands data privacy regimes that are interoperable.

The APEC Cross-Border Privacy Rules System, with which some of you may be familiar, is an attempt to create a voluntary and interoperable system that provides meaningful safeguards for consumer data. Privacy authorities, businesses, and civil society groups in the APEC region negotiated detailed privacy rules ð the APEC Cross-Border Privacy Rules or ñCBPRsò ð based on nine high-level privacy principles. Businesses that want to participate in the CBPRs will submit their privacy policies and practices for review and certification by third-

Ministers last November, and the system is set to launch this year. The United States applied to participate in the system just last month.

I have been personally involved in developing the system since joining the FTC two years ago, along with other FTC and U.S. Department of Commerce staff. The privacy and legal regimes in the vast APEC region vary widely. But despite those differences, APEC members have come together to develop a system that reflects a consensus on what constitutes sound cross-border data protection. This approach of agreeing on common rules to which individual companies can pledge their adherence and that are enforceable in all participating economies represents an important way to bridge differences across jurisdictions.

Of course, I also recognize that not all companies will meaningfully embrace privacy by design. Many companies face intense pressure to maximize profits from the use of consumer data, and some believe that giving consumers choices about their data will limit that profit potential. In my view, that is a short-sighted approach that ignores the benefit